UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

ALLERGAN, INC., ALLERGAN PHARMACEUTICALS IRELAND, UNLIMITED COMPANY, ALLERGAN USA, INC., AND ALLERGAN SALES, LLC	)	
Plaintiffs,	)	Civil Action No. 3:23-cv-00431
	)	Judge Richardson/Frensley
v.	)	
	)	
REVANCE THERAPEUTICS, INC.	)	
Defendant.	)	

ORDER OF THE SPECIAL MASTER RESOLVING PLAINTIFFS' MOTION TO COMPEL SEARCHING OF DEVICES USED UNDER REVANCE'S BYOD POLICIES

This case comes before the Special Master on Plaintiffs' Motion to Compel Searching of Devices Used Under Revance's BYOD Policies (ECF 255) (the "Motion"). Upon consideration of the sealed brief in support (ECF 240),[1] the response in opposition (ECF 268), the relevant sealed position statement of the parties (ECF 238), and the relevant exhibits the parties submitted (ECF 241; ECF 242; ECF 255-2; ECF 255-5; ECF 255-6; ECF 255-7; ECF 255-8; ECF 269-1; ECF 269-2), the Special Master **DENIES** the Motion.

I. General Background

This is a trade secrets misappropriation case. Two classes of cosmetic products are at issue: (1) biologic therapeutics employing botulinum neurotoxin ("BoNT") and (2) dermal fillers. Plaintiffs (various entities doing business under the "Allergan" trade name)[2] allege that Defendant Revance Therapeutics, Inc.[3] misappropriated trade secrets related to Plaintiffs' popular products

[1] Because Revance is not seeking to seal Exhibits A or B to the Declaration of Jennifer Baldocchi (ECF 255-2 ¶¶ 2–3; ECF 241; ECF 242), *see* ECF 270 at 1, the Special Master cites to and discusses herein portions of the sealed brief in support that reference these exhibits.

[2] This Order refers to Plaintiffs as "Plaintiffs" and "Allergan" interchangeably.

[3] This Order refers to Defendant as "Defendant" and "Revance" interchangeably.

Botox (a BoNT therapeutic) and Juvéderm (a dermal filler). *See, e.g.*, Compl. (ECF 1) ¶ 1. Defendant allegedly accomplished this misappropriation by hiring Allergan employees and, presumably, encouraging them to take Plaintiffs' trade secrets with them. *See, e.g.*, *id.* ¶¶ 7–8, 10, 75, 87.

Discovery in this case has been lengthy. The parties have been conducting discovery pursuant to an agreed Joint Discovery Plan (ECF 90; ECF 223), which provides a framework for, among other things, the production of electronically stored information ("ESI").[4] Despite the parties' agreement on that basic framework, various discovery disputes have ensued.

On July 14, 2023, Allergan served its First Set of Requests for Production on Revance. (ECF 255-2 ¶ 11; ECF 255-8). Among other requests, Allergan requested that Revance produce documents responsive to the following categories:

- **RFP No. 14:** All communications between any current or former Allergan employee, including, but not limited to, the individuals listed in [the list of employees who left Allergan for Revance], and Revance referencing Allergan.
- **RFP No. 18:** All Allergan documents that Revance has in its possession, custody, or control.
- **RFP No. 19:** All documents that Revance has in its possession, custody, or control that contain Allergan information.
- **RFP No. 87:** Documents sufficient to identify each customer of DaxibotulinumtoxinA for Injection in the United States.

(ECF 240 at 2; ECF 255-8 at 3–4).

On November 15, 2024, the parties jointly moved the Court to "appoint a discovery special master to resolve discovery disputes," "[g]iven the number of discovery disputes currently pending

[4] The parties Joint Discovery Plan does not displace the background ESI principles of the Middle District's Administrative Order 174-1. *See* ECF 90 ¶ 8(a) ("This ESI Protocol [within the Joint Discovery Plan] applies to the ESI provisions of Federal Rules of Civil Procedure 26, 33, 34, and 37, and Administrative Order 174-1 of the U.S.D.C. Middle District of Tennessee."); (ECF 223 ¶ 8(a) (same)).

before the Court and the number of disputes expected to be raised in the future based on the parties' discussions." (ECF 271 ¶ 6). The Court granted that request on November 18, 2024, stating that it would appoint a special master to rule on "all discovery matters currently pending before the Court, and all future discovery disputes." (ECF 275 ¶ 1). On December 11, 2024, the Court appointed the undersigned as Special Master. (ECF 292).

II. Issues Raised by the Motion

The Motion concerns Allergan's request to compel Revance to search the personal devices of four individuals for documents responsive to Allergan's discovery requests.[5] These four individuals are Alexis Jammo, Domenico Vitarella, Todd Gross, and Roy Yoshimitsu, all of whom previously worked for Allergan and then worked for Revance. Each of these individuals used his or her personal devices while working for Revance pursuant to Revance's Mobile Device Policy, or "Bring Your Own Device" policy ("BYOD Policy"). (ECF 255-5 at 2; ECF 255-6 at 2). Allergan contends that the BYOD Policy (ECF 269-2) and the Revance Employee Handbook ("Handbook") (ECF 269-1), when read in tandem, support compelling Revance to search its employees' personal devices. Revance disagrees that it has possession, custody, or control over its employees' personal devices used pursuant to the BYOD Policy and raises privacy concerns.[6]

---

[5] Allergan contends that RFPs 14, 18, 19 and 87 are "just a few examples" of requests for which responsive documents "will be found on the devices of the former Allergan employees at issue here." (ECF 240 at 2).

[6] Allergan generally asserted that discovery of Revance employees' personal devices is proportional to the needs of the case (ECF 240 at 1) and Revance did not argue otherwise, (ECF 268, *passim*), so the Special Master assumes for purposes of this Order that the discovery falls within Rule 26's proportionality standard. Moreover, the parties' briefing indicates that Allergan chose not to issue Rule 45 subpoenas directly to the subject employees and this Order therefore addresses only whether Revance has sufficient Rule 34(a) control over its employees' personal devices to require it to obtain and produce data from those personal devices. *See Halabu Holdings, Inc. v. Old Nat'l Bancorp*, No 20-10427, 2020 WL 12676263, at *3 (E.D. Mich. June 9, 2020) (noting that, "[o]f course, personal devices owned by non-defendant employees are not immunized from discovery," that, "[l]ike most other sources of information, they can be reached by way of a

A. Relevant Excerpts from the Handbook

The Revance Handbook "is intended to give [employees] the framework and guidelines that should assist [them] in the performance of [their] job and the accomplishment of [their] goals." (ECF 269-1 at 2). Under the heading "COMPANY PROPERTY," the Handbook contains a "Search Policy" section. *Id.* at 48–49. The "Search Policy" section describes "Company property" and Revance's inspection rights associated with Company property. *Id.* According to this policy,

> Furniture, desks, computers, cell phones, data processing equipment/software, vehicles, and other company-owned items are Company property and must be maintained according to Company rules and regulations . . . . The Company reserves the right to inspect all Company property including computer or phone data or messages to ensure compliance with its rules and regulations, without notice to the employee and at any time, not necessarily in the employee's presence. There is no expectation of privacy in the possession or use of any Company property.

Id. at 48.

The Handbook also contains an "Electronic and Social Media" section. *Id.* at 49–50. The section starts with several definitions, including,

> "Computers" are defined as . . . handheld devices (including but not limited to smart phones, and other electronic tablets and cell phones) . . . and other Company-owned items.
> . . .
> "Electronic communication" includes e-mail, text messages, telephones, cell phones and other handheld devices (such as cell phones, smart phones or electronic tablets) . . . .
>
> "Electronic information" is any information created by an employee using computers or any means of electronic communication, including but not limited to, data, messages, multimedia data, and files.

Id. at 49. The section continues with some general policies, including:

- Computers and all data transmitted through Company servers are Company property owned by the Company for the purpose of conducting Company business . . . .

---

subpoena under Rule 45 of the Federal Rules of Civil Procedure," and that, "[b]ecause [the requesting party] did not choose the Rule 45 subpoena route, it bears the burden of establishing [the responding party's] control over the devices").

- All electronic communications also remain the sole property of the Company and are to be used for Company business. For example, e-mail messages are considered Company records.

- Electronic information created by an employee using any computer or any means of electronic communication is also the property of the Company and remains the property of the Company.

Id. at 49–50.

Finally, as for monitoring company property, the Handbook notes that:

> The Company reserves the right to inspect all Company property to ensure compliance with its rules and regulations, without notice to the employee and at any time, not necessarily in the employee's presence. Company computers and all electronic communications and electronic information are subject to monitoring, and no one should expect privacy regarding such use. The Company reserves the right to access, review and monitor phone calls, electronic files, information, messages, text messages, e-mail, Internet history, browser-based webmail systems and other digital archives and to access, review and monitor the use of computers, software, and electronic communications to ensure that no misuse or violation of Company policy or any law occurs. E-mail may be monitored by the Company and there is no expectation of privacy.

Id. at 50.

B. Relevant Excepts from the BYOD Policy

Revance's BYOD Policy states that its purpose "is to outline the acceptable use of both Revance-Owned mobile devices and personal mobile devices." (ECF 269-2 at 1, § 1.0). The policy defines "Revance-Owned" as a "[m]obile device that is 100% paid (Hardware and Service) for by Revance[,]" *id.* at 2, § 5.1, a personal mobile device as "a mobile device which is not provided by Revance and is used to connect to Revance Information Technology systems," *id.* § 5.2, and "acceptable use" as "activities that directly or indirectly support the business of Revance." *Id.* at 4, § 6.2.1. Revance's BYOD Policy permits Revance personnel to use their personal mobile devices so long as they "adhere to a minimum IT standard to access Revance email system and the Revance wireless network as necessary in the course of their normal business routines in support of Revance goals and objectives." *Id.* at 3, § 6.1.1. Revance personnel must agree to a general code

of conduct to protect the confidentiality of the company's data, including keeping the operating system and device current "with security patches and updates," *id.* § 6.1.4.3, refraining from copying personal or sensitive business data from company applications to an unauthorized application or an unapproved personal device, *id.* at 3–4, § 6.1.4.4, "[c]onducting Revance business on the mobile device only via the user's Revance email account and Revance IT approved email application," *id.* at 4, § 6.1.4.6, and allowing an inspection of the "device configuration to ensure compliance with all applicable Revance information security policies." *Id.* § 6.1.4.9. The policy identifies three situations under which "[t]he mobile device may be remotely wiped": (1) "[t]he device is lost[;]" (2) "IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure[;]" or (3) "[a]ny user with an active IT account and has departed Revance." *Id.* at 7, §§ 6.5.5, 6.5.5.1, 6.5.5.2, 6.5.5.3.

III. Discussion

Allergan seeks to compel Revance to produce data contained on the personal devices of four current or former employees: Alexis Jammo, Domenico Vitarella,[7] Todd Gross,[8] and Roy

[7] Mr. Vitarella is no longer a Revance employee (ECF 255-6 at 2), but the Special Master will not differentiate Mr. Vitarella from the three current Revance employees because Mr. Vitarella was a Revance employee at the time Allergan served its requests (ECF 240 at 13).

[8] The parties disagree as to whether Mr. Gross is an appropriate ESI custodian, and this topic was the subject of two prior motions before the Special Master. As explained in the Order of the Special Master Resolving Plaintiffs' Renewed Motion to Compel Production of Certain Documents (ECF 302) and Order of the Special Master Resolving Plaintiffs' Motion to Compel Searching of ESI Custodians (ECF 303), Plaintiffs did not demonstrate that Mr. Gross was an appropriate ESI custodian because Plaintiffs failed to sufficiently explain why it believes Mr. Gross might possess unique, discoverable ESI. (ECF 302 at 18–19; ECF 303 at 3–4); *see Mortg. Resol. Servicing, LLC v. JPMorgan Chase Bank, N.A.*, 15 CV 0293, 2017 WL 2305398, at *3 (S.D.N.Y. May 18, 2017). Thus, regardless of the outcome of this Motion, Revance would not be required to search Mr. Gross's personal device because he is not a proper custodian. Regardless, the reasons for denying Plaintiffs' request to compel a search of personal devices apply to Mr. Gross.

Yoshimitsu. Allergan does not claim that Revance has actual possession or custody of these personal devices but argues that Revance has "control" over those devices within the meaning of Federal Rule of Civil Procedure 34(a). For the reasons explained below, the Special Master finds that Revance does not have Rule 34(a) control over these employees' personal devices and, as such, the Special Master denies the Motion.

A. Legal standard under Rule 34

Pursuant to Federal Rule of Civil Procedure 34, "[a] party may serve on any other party a request within the scope of Rule 26(b): to produce and permit the requesting party or its representative to inspect, copy, test, or sample the following items in the responding party's possession, custody, or control[.]" Fed. R. Civ. P. 34(a)(1). Courts across the country have generally applied two standards when determining whether a responding party has Rule 34(a) control over the requested information: the "legal right" standard and the "practical ability" standard.

Courts applying the "legal right" standard assess whether the responding party "has the legal right to obtain the documents on demand from someone else," which is "understood to include 'the legal right to command release from the party with actual possession.'" *Halabu Holdings, LLC v. Old Nat'l Bancorp*, No. 20-10427, 2020 WL 12676263, at *3 (E.D. Mich. June 9, 2020) (quoting *Hayse v. City of Melvindale*, No. 17-13294, 2018 WL 3655138, at *6 (E.D. Mich. Aug. 2, 2018), *objections overruled*, No. 17-13294, 2018 WL 4961528 (E.D. Mich. Oct. 15, 2018)); *see also J.S.T. Corp. v. Robert Bosch LLC*, No. 15-13842, 2019 WL 2354631, at *6 (E.D. Mich. June 3, 2019) ("The Legal Right Standard 'requires a party to preserve, collect, search, and produce Documents and ESI which the party has a legal right to obtain.'") (quoting The Sedona Conference, *The Sedona Conference Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control"*, 17 SEDONA CONF. J. 467, 484 (2016)). Stated differently, "[d]ocuments are not

discoverable under Rule 34 if the entity that holds them 'could legally—and without breaching any contract—continue to refuse to turn over such documents.'" *Matthew Enter., Inc. v. Chrysler Grp. LLC*, No. 13-cv-04236-BLF, 2015 WL 8482256, at *3 (N.D. Cal. Dec. 10, 2015) (quoting *In re Citric Acid Litig.*, 191 F.3d 1090, 1108 (9th Cir. 1999)). In concluding that the "legal right" approach was proper (or the "legal control test" as the judges referred to it), the Ninth Circuit noted that "[o]rdering a party to produce documents that it does not have the legal right to obtain will oftentimes be futile, precisely because the party has no certain way of getting those documents." *In re Citric Acid Litig.*, 191 F.3d at 1108.

Other courts "have adopted a more expansive notion of 'control,' finding that it extends to circumstances where a party has the 'practical ability to obtain the documents from a nonparty to the action.'" *Flagg v. City of Detroit*, 252 F.R.D. 346, 353 n.16 (E.D. Mich. 2008) (quoting *Bank of New York v. Meridien BIAO Bank Tanzania Ltd.*, 171 F.R.D. 135, 146 (S.D.N.Y. 1997)). While this "practical ability" standard lacks a precise definition, *see* The Sedona Conference, *supra*, at 499–500 (surveying cases), courts utilizing this standard focus on the responding party's relationship with the non-party owner of the requested information, including whether the responding party considers the requested information to be records that it requests and obtains in the ordinary course of business, whether the case history demonstrates the non-party's cooperation in producing documents or otherwise assisting in discovery, and whether the non-party has a personal financial interest in the litigation's outcome. *See St. Clair Cnty. Emps. Ret. Sys. v. Acadia Healthcare Co.*, No. 3:18-cv-00988, 2022 WL 4095387, at *10 (M.D. Tenn. Sept. 7, 2022), *aff'd*, 2023 WL 3659734 (M.D. Tenn. May 25, 2023); *Gross v. Lunduski*, 304 F.R.D. 136, 142 (W.D.N.Y. 2014); *Libertarian Party of Ohio v. Husted*, No. 2:13-CV-953, 2014 WL 3928293, at *1–2 (S.D. Ohio Aug. 12, 2014); *Afremov v. Sulloway & Hollis, P.L.L.C.*, No. 09-cv-03678, 2011 WL 13199154, at *2 (D. Minn. Dec. 2, 2011).

The Sixth Circuit, in *In re Bankers Trust Co.*, stated that "federal courts have consistently held that documents are deemed to be within the 'possession, custody or control' for purposes of Rule 34 if the party has *actual* possession, custody or control, or has the legal right to obtain the documents on demand." 61 F.3d 465, 469 (6th Cir. 1995) (emphasis in original) (citing *Resolution Trust Corp. v. Deloitte & Touche*, 145 F.R.D. 108, 110 (D. Colo. 1992); *Weck v. Cross*, 88 F.R.D. 325, 327 (N.D. Ill. 1980)). Some courts and commentators interpret this statement as the Sixth Circuit's adoption of the "legal right" standard. *See, e.g.*, *Halabu Holdings, LLC v. Old Nat'l Bancorp*, No. 20-10427, 2020 WL 12676263, at *3 (E.D. Mich. June 9, 2020) (identifying "the principle enunciated in *In re Bankers Trust Co.*" as requiring "that the party served with the document request 'has the legal right to obtain the documents on demand' from someone else"); *J.S.T. Corp. v. Robert Bosch LLC*, No. 15-13842, 2019 WL 2354631, at *6 (E.D. Mich. June 3, 2019) ("Courts in the Sixth Circuit have adopted the Legal Right Standard . . . ."), *report and recommendation adopted*, No. 15-13842, 2019 WL 2343705 (E.D. Mich. June 3, 2019); *Pasley v. Caruso*, No. 10-CV-11805, 2013 WL 2149136, at *5 (E.D. Mich. May 16, 2013) (noting, as to the "practical ability" standard, that "the Sixth Circuit has not adopted this 'expansive notion of control'"); *Flagg v. City of Detroit*, 252 F.R.D. 346, 353 (E.D. Mich. 2008) ("The Sixth Circuit and other courts have held that documents are deemed to be within the 'control' of a party if it 'has the legal right to obtain the documents on demand.'"); The Sedona Conference, *supra*. (concluding that the Sixth Circuit follows the "legal right" standard).

Yet, "[o]ther courts within the Sixth Circuit have found that 'control' includes the practical ability to produce documents from a third party." *St. Clair Cnty. Emps. Ret. Sys. v. Acadia Healthcare Co., Inc.*, No. 3:18-cv-00988, 2022 WL 4095387, at *9 (M.D. Tenn. Sept. 7, 2022), *aff'd*, No. 3:18-cv-00988, 2023 WL 3659734, at *3 (M.D. Tenn. May 25, 2023) (stating that, "[i]mportantly, *Bankers Trust* does not limit 'control' to only that which a party has a legal right

to obtain" and acknowledging that, "[t]o be sure, some district courts within the Sixth Circuit have applied the 'legal right' test; but courts within the Circuit have also found that 'control' includes the practical ability to obtain documents from a third party"); *see also Union Com. Servs. Ltd. v. FCA Int'l Operations LLC*, No. 16-cv-10925, 2018 WL 558760, at *2 (E.D. Mich. Jan. 25, 2018) ("[D]iscovery material is within a party's control when the party has the 'practical ability to obtain the documents, particularly when the opposing party does not have the same practical ability to do so.'") (*quoting S2 Automation, LLC v. Micron Tech., Inc.*, No. CIV 11–0884, 2012 WL 3656454, at *33 (D.N.M. Aug. 9, 2012)).

Within these varying applications of Rule 34(a) "control" standards, relatively few courts have addressed whether to apply the "legal right" standard or "practical ability" standard in the context of an employer's Rule 34(a) control over its employees' personal devices, such as cell phones or tablets. In this context, the court's decision in *In re Pork Antitrust Litigation*, No. 18-cv-1776, 2022 WL 972401 (D. Minn. Mar. 31, 2022), is instructive.

In the *Pork Antitrust* class-action case, the class plaintiffs sought to compel defendant Hormel Foods Corporation to produce text-message content from its employees' personally owned cell phones. 2022 WL 972401, at *3. Hormel claimed that its employees' personal cell phones were beyond its Rule 34(a) control, but the plaintiffs disagreed, citing Hormel's BYOD policy. *Id.* at *3, *4. The BYOD policy allowed Hormel's employees to use personally owned cell phones to interact with its corporate systems and claimed ownership of data that the cell phones sourced from these systems, including company email, calendars, and contacts, but excluding text messages. *Id.* at *5. The policy permitted Hormel to remotely remove company data from employees' cell phones but did not allow Hormel to access or search text messages. *Id.*

In determining whether Hormel had Rule 34(a) control over its employees' cell phones, the court noted that the Eighth Circuit had not ruled on the appropriate standard and that district courts

within the Circuit had applied "varying definitions of 'control,'" *id.* at *3, including the "legal right" standard and the "practical ability" standard. *Id.* at *3–4 (collecting cases). The court recognized criticisms of the "practical ability" standard, including that its imprecise definition "has resulted in inconsistent and, at times, inequitable results," *id.* at *4 (citing The Sedona Conference, *supra*, at 528), and that, even if a court were to order an employer to produce its employees' personal emails, there must be some "authority under which the employer could force the employees to turn them over." *Id.* at *4 (citing *Matthew Enter., Inc. v. Chrysler Group LLC*, No. 13-cv-04236-BLF, 2015 WL 8482256 (N.D. Cal. Dec. 10, 2015)). On the latter point, the court questioned the "practical ability" standard in the employer–employee context, stating:

> It is one thing to show that a responding party may *ask* for documents in the possession of someone with whom it has a relationship, but quite another to conclude that the party has the practical ability to *demand* such documents, and therefore has "control" over them. The Court is particularly sensitive to this distinction in the context of the employment relationship. While one might argue that the employees' fear for their job security or interest in the financial well-being of the company will incentivize them to say "yes" to turning over their text messages for inspection and possible production is not, in the opinion of the undersigned, the kind of "practical ability" contemplated by the standard.

Id. at *6 (D. Minn. Mar. 31, 2022).

The court ultimately determined that it would not select a particular standard because the plaintiffs failed to show that Hormel had any control, legally or practically, to obtain and produce data from its employees' cell phones. Even though Hormel's BYOD policy claimed ownership of "all data sourced from Hormel," it did not "explicitly assert ownership, control, or the ability to access, inspect, copy, image, or limit personal text messages," nor did it require "any employee who uses a personally-owned cell phone to use text messaging to conduct work." *Id.* at *5. As a result, the court held that Hormel's BYOD policy did not give it "control over the text messages on personally-owned cell phones." *Id.* at *6.

The *Pork Antitrust* decision finds support within the Sixth Circuit via the court's decision in *Halabu Holdings, LLC v. Old National Bancorp*, No. 20-10427, 2020 WL 12676263 (E.D. Mich. June 9, 2020). In *Halabu Holdings*, the plaintiff moved to compel the defendant bank to produce data from its employees' personal cell phones. *Id.* at *1. Raising concerns about the employees' privacy and property rights associated with their personal cell phones, the court followed the "legal right" standard, which required proof of "the legal right to command release from the party with actual possession." (*quoting Hayse v. City of Melvindale*, No. 17-13294, 2018 WL 3655138, at *6 (E.D. Mich. Aug. 2, 2018)). While recognizing that employers and employees may agree that the employer may search or access their personal devices, the court found that the plaintiff failed to show an agreement, policy, or practice showing that the bank had control over its employees' devices. *Id.* at *3. As such, it found no Rule 34(a) control and denied plaintiff's motion to compel. *Id. See also Matthew Enter., Inc. v. Chrysler Group LLC*, No. 13-cv-04236-BLF, 2015 WL 8482256 (N.D. Cal. Dec. 10, 2015) (applying the "legal right" standard and denying requesting party's attempt to obtain personal email accounts of the responding party's employees); The Sedona Conference, *supra*, at 527 (recommending the "legal right" standard over the "practical ability" standard and concluding that, "[w]ithout the employee's consent, an employer is not likely to have the legal right to both secure control and custody of the device, much less preserve information on the same device").

The Special Master finds persuasive the reasoning of courts' decisions in *Pork Antitrust Litigation* and *Halabu Holdings* as well as the recommendation of The Sedona Conference,[9] and

[9] Courts often find persuasive principles enunciated by the Sedona Conference in discovery issues. *See, e.g.*, *M.A. v. Wyndham Hotels & Resorts, Inc.*, Nos. 2:19-cv-849, 2:19-cv-755, 2020 WL 1983069, at *4 (S.D. Ohio Apr. 27, 2020) ("Courts in the Sixth Circuit have relied on the Sedona Principles to inform their analysis of ESI discovery requests."); *LKQ Corp. v. Kia Motors Am.*, 345 F.R.D. 152, 162 (N.D. Ill. 2023) ("To address disputes regarding ESI, many courts have also turned to the Sedona Principles and Sedona Commentaries, which are 'the leading authorities

will apply the "legal right" standard to determine whether an employer (Revance) has Rule 34(a) control over its employees' personal devices. Allergan bears the burden to prove Revance's legal right to obtain and produce information from its employees' personal devices, *Halabu Holdings*, 2020 WL 12676263, at *3, and asserts that "Revance has the legal right to obtain electronic communications stored on its employees' personal email or text messaging applications because they were used for work-related purposes." (ECF 240 at 8).[10] Allergan, however, cited no authority for the proposition that an employer has a "legal right" to its employees' personal devices simply because the employees may use those devices for work-related purposes, and the cases otherwise cited in support (ECF 240 at 8–9) are inapposite:

- In *State Farm Mut. Auto. Ins. Co. v. Precious Physical Therapy, Inc.*, defendants did not issue email addresses to their employees or independent contractors, nor did the court analyze a BYOD policy. No. 19-10835, 2020 WL 7056039, at *2 (E.D. Mich. Dec. 2, 2020). While the court ordered defendants to produce responsive emails in the employees' possession, *id.* at *6, the Special Master understands that Revance has already searched, or is in the process of searching, for responsive emails in its employees' Revance email accounts.[11]

- *Bloomer v. Word Network Operating Co., Inc.* is unhelpful because while defendants expressed concern over producing personal text messages, there is no analysis of a BYOD policy or what might give the employer "possession, custody, or control" over email accounts. No. 22-12433, 2023 WL 8540000 (E.D. Mich. Dec. 8, 2023).

- *Union Home Mortg. Corp. v. Jenkins* involved a motion to compel as to a non-party subject to a Rule 45 subpoena. No. 1:20cv2690, 2021 WL 1110440, at *1 (N.D. Ohio

---

on electronic document retrieval and production.'") (quoting *DeGeer v. Gillis*, 755 F. Supp. 2d 909, 918 (N.D. Ill. 2010)).

[10] Allergan cites to paragraph 6 of the Baldocchi Declaration to support its factual claims "(1) that Revance employees have admitted to using their personal phones to communicate about business and (2) that the devices of some Revance employees have already been found to contain evidence of misappropriation." ECF 240 at 7. But paragraph 6 of the Baldocchi Declaration simply summarizes a meeting between counsel regarding "the devices used pursuant to the BYOD Policy and Employee Handbook," "concerns about the burden of investigating so many individuals" by Revance's counsel, and Allergan's limitation of "the individuals whose devices it believed should be searched to the Former Allergan Employees it believed likely to have relevant evidence." ECF 255-2 ¶ 6. This paragraph does not support the proposition cited to in the brief.

[11] Again, other than Mr. Gross.

Mar. 23, 2021). Notably, because the defendant had received a responsive video text message from the non-party, the court ordered the non-party "to ask its current employees to search for and provide for production all relevant emails and text messages in their personal email and cell phone accounts which are responsive to Request Numbers 4 and 10." *Id.* at *10. Here, Allergan has provided no evidence indicating that any of the proposed custodians used any mobile applications other than email for work.

- *Wiginton v. Metro. Nashville Airport Auth.* is easily distinguishable, as the defendant in that case was subject to the Tennessee Public Records Act ("TPRA"), so it had "a legal right to obtain the requested communications because it [was] required by the TPRA to disclose public records that are not otherwise exempt." No. 3:17-cv-01523, 2019 WL 12096809, at *2, *4 (M.D. Tenn. May 31, 2019). No such legal right exists here.

- *ID Ventures, LLC v. Chubb Custom Ins. Co.* concerned searching employee email accounts for responsive documents and did not address personal devices or whether the employer would have a legal right to search those devices. No. 17-14182, 2018 WL 8807125, at *2 (E.D. Mich. Oct. 12, 2018).

Although Allergan did not assert that Revance's Handbook or BYOD policy gave Revance the "legal right" to obtain its employees' personal devices, it argued, without citation to any specific legal standard, that Revance had control over its employees' personal devices through its Handbook and BYOD devices. (ECF 240 at 10–12). For the reasons explained below, the Special Master disagrees.

B. The Handbook

According to Allergan, the Handbook's "Cell Phone Policy" supports its argument that Revance has control over the employees' personal devices. (ECF 240 at 11). But Revance correctly points out that this policy is "aimed at employee safety" and prohibiting employees from using their cell phones to conduct business while driving. (ECF 268 at 6). As such, the Handbook's "Cell Phone Policy" does not establish Revance's control over its employees' personal devices.

Allergan also argues that the "Electronic and Social Media" policy "governs not only 'Company-owned' computers, but also various forms of 'electronic communication[.]'" ECF 240 at 11. Revance counters that "the policy limits Revance's ability to inspect only '***Company***

property.'" (ECF 268 at 7) (citing ECF 269-1 at 50). The Special Master agrees with Revance. The Handbook's definition of "Computers" includes "desktop computers, laptops, handheld devices (including but not limited to smart phones, and other electronic tablets and cell phones) . . . *and other Company-owned items.*" (ECF No. 269-1 at 49) (emphasis added). The inclusion of "other *Company-owned* items" plainly demonstrates that the definition refers to only Company-owned cell phones. Moreover, the inclusion of "cell phone" in the definition of "[e]lectronic communication" does not transform the definition of "Computers" to include personal cell phones. As such, the Handbook, standing alone, provides insufficient support for holding that Revance has the required Rule 34(a) control over its employees' personal devices, such that Revance should be compelled to search their devices.

C. BYOD Policy

The BYOD Policy—whether standing alone or read in tandem with the Handbook—also does not support Allergan's arguments. Revance has had the BYOD Policy in place since March 2019 to govern "the acceptable use of both Revance-Owned mobile devices and personal mobile devices." (ECF 269-2 at 1, § 1). Pursuant to this BYOD Policy, "Revance personnel may use mobile devices that adhere to a minimum IT standard to access Revance email system and the Revance wireless network as necessary in the course of their normal business routines in support of Revance goals and objectives." *Id.* at 3, § 6.1.1.

Allergan cites various provisions of the BYOD Policy to argue that these provisions, when read together with the Handbook, give Revance control of the employees' personal devices and allow Revance to search them. (ECF 240 at 10–12). Revance argues in response that the BYOD Policy "is not as sweeping as Allergan claims" and that it permits employees to conduct business on their personal devices only through their email account. (ECF 268 at 7–8).

The Special Master agrees with Revance. Just as in the BYOD policy in the *Pork Antitrust* case, Revance's BYOD Policy does not authorize a search of its employees' personal devices for any reason other than to inspect the "device configuration to ensure compliance with all applicable Revance information security policies." (ECF 269-2 at 4, § 6.1.4.9). Moreover, the BYOD Policy is clear that the "code of conduct includes agreement to: . . . [c]onduct Revance Business on the mobile device only via the user's Revance email account and Revance IT approved email application." (*Id.* § 6.1.4.6). As mentioned, Revance has already searched and agreed to produce company emails for each of the relevant custodians.[12] But the Motion seeks the production of information *beyond* email, such as text messages. The BYOD Policy plainly forbidding the use of personal devices to conduct Revance business in applications other than email militates against a finding that Revance has Rule 34(a) control of those other applications.

While the Special Master adopts and applies the "legal right" standard where a party seeks to compel an employer to produce information contained on its employees' personal devices, the Special Master further rules that Revance does not have Rule 34(a) control over its employees' devices under the "practical ability" standard. Here, to the extent Allergan even argues that Revance's Handbook and BYOD policy give it the "practical ability" to search for, collect, and produce information on its employees' personal devices, for the same reasons that Revance does not have the legal right to require its employees to produce their personal-device data, the Special Master finds that Revance does not have the practical ability to force its employees to produce their personal devices for inspection. Moreover, Allergan did not argue or otherwise establish that Revance obtains its employees' personal-device data in the ordinary course of business, or that the Revance employees from whom personal devices are sought have cooperated in producing

[12] Other than Mr. Gross, who is not a valid custodian. (ECF 302 at 18–19; ECF 303 at 3–4).

documents or have a financial interest in this litigation. *St. Clair Cnty. Emps. Ret. Sys. v. Acadia Healthcare Co.*, No. 3:18-cv-00988, 2022 WL 4095387, at *10 (M.D. Tenn. Sept. 7, 2022), *aff'd*, 2023 WL 3659734 (M.D. Tenn. May 25, 2023).

Accordingly, without an agreement between Revance and its employees permitting Revance to search employees' personal devices, explicit language in the policy giving Revance control over its employees' personal-advice data, or more information about whether the subject employees actually used any other application on their personal phones for work purposes, the Special Master finds that Revance does not have Rule 34(a) control over the personal devices of employees Alexis Jammo, Domenico Vitarella, Todd Gross, and Roy Yoshimitsu.

IV. Conclusion

In accordance with the foregoing, the Special Master hereby **ORDERS** that:

1. Plaintiffs' Motion to Compel Searching of Devices Used Under Revance's BYOD Policies (ECF 255) is **DENIED**.

2. Pursuant to paragraph three of the Court's Order Modifying Case Management Order and Granting Request for the Appointment of a Special Master (ECF 275), the parties have twenty-one (21) days from the date of this Order to file objections or a motion to adopt or modify any of the Special Master's rulings in this Order.

IT IS SO ORDERED.

Signed March 17, 2025.

s/ Todd Presnell
Special Master Todd Presnell